

k -anonymous Microdata Release via Post Randomisation Method

Dai Ikarashi, Ryo Kikuchi, Koji Chida, and Katsumi Takahashi

NTT Secure Platform Laboratories,
 {ikarashi.dai, kikuchi.ryo, chida.koji, takahashi.katsumi}@lab.ntt.co.jp

Abstract. The problem of the release of anonymized microdata is an important topic in the fields of statistical disclosure control (SDC) and privacy preserving data publishing (PPDP), and yet it remains sufficiently unsolved. In these research fields, k -anonymity has been widely studied as an anonymity notion for mainly deterministic anonymization algorithms, and some probabilistic relaxations have been developed. However, they are not sufficient due to their limitations, i.e., being weaker than the original k -anonymity or requiring strong parametric assumptions. First we propose Pk -anonymity, a new probabilistic k -anonymity, and prove that Pk -anonymity is a mathematical extension of k -anonymity rather than a relaxation. Furthermore, Pk -anonymity requires no parametric assumptions. This property has a significant meaning in the viewpoint that it enables us to compare privacy levels of probabilistic microdata release algorithms with deterministic ones. Second, we apply Pk -anonymity to the post randomization method (PRAM), which is an SDC algorithm based on randomization. PRAM is proven to satisfy Pk -anonymity in a controlled way, i.e., one can control PRAM's parameter so that Pk -anonymity is satisfied. On the other hand, PRAM is also known to satisfy ϵ -differential privacy, a recent popular and strong privacy notion. This fact means that our results significantly enhance PRAM since it implies the satisfaction of *both* important notions: k -anonymity and ϵ -differential privacy.

Keywords: Post Randomization Method (PRAM), k -anonymity, differential privacy

1 Introduction

Releasing microdata while preserving privacy has been widely studied in the fields of statistical disclosure control (SDC) and privacy preserving data publishing (PPDP). Microdata has significant value, especially for data analysts who wish to conduct various type of analyses involving the viewing of whole data and determining what type of analysis they should conduct.

The most common privacy notion for microdata release is *k-anonymity* proposed by Samarati and Sweeney [18, 20]. It means that “no one can narrow down a person’s record to k records.” This semantics is quite simple and intuitive. Therefore, many studies have been conducted on k -anonymity, and many relevant privacy notions such as ℓ -diversity [13], have also been proposed. Among these relevant studies, applying k -anonymity to probabilistic algorithms is a significant research direction. Most k -anonymization algorithms deterministically generalize or partition microdata. However, there are probabilistic SDC methods such as random swapping, random sampling, and post randomization method (PRAM) [9]. How are these probabilistic algorithms related to k -anonymity?

Regarding random swapping, for example, Soria-Comas and Domingo-Ferrer answered the above question by relaxing k -anonymity to a probabilistic k -anonymity, which means that “no one can *correctly link* a person to a record with a higher probability than $1/k$ [19].” Intuitively, this semantics seems to be very close to that of the original k -anonymity. However, its precise relation to k -anonymity has not been argued, and we still cannot definitely say that an algorithm satisfying their probabilistic k -anonymity also is k -anonymous.

PRAM was proposed by Kooiman et al. in 1997. It changes data into other random data according to the probability on a *transition probability matrix*. Agrawal et al. also developed privacy preserving OLAP (Online Analytical Processing) [3] by retention-replacement perturbation, which is an instantiation of PRAM. For many years, PRAM’s privacy was not clarified; however, PRAM has been recently proven to satisfy ϵ -differential privacy (DP) [12].

Differential privacy [6] is another privacy notion that has attracted a great deal of attention recently. ϵ -DP is the original version of DP and many other relevant notions have been developed, e.g., (ϵ, δ) -DP, which is a relaxation of ϵ -DP.

1.1 Motivations

After the proposal, ϵ -DP has been widely researched and is now known to be very strong privacy notion. Thus, it is natural that the satisfaction of ϵ -DP is important. However, especially in the PPDP field, k -anonymity is as important as ϵ -DP, although it takes only re-identification into consideration and several papers showed the limitation of k -anonymity [13, 10]. This notion is very simple and intuitive; therefore, the enormous number of techniques has been invented, and as a result, k -anonymity has already spread among the businesspeople, doctors, etc., who are conscious about privacy, not only among the researchers. From the viewpoint of practice, it is a great merit that people recognize and understand the notion.

Therefore, merging the two notions while preserving their theoretical guarantees in a controlled way is desirable. However, k -anonymity applies only to deterministic anonymization algorithms, and ϵ -DP applies to randomized ones; thus, it has been hard to manage both of them at once until now.

PRAM has several good features, and we believe that it is one of promising candidates for PPDP. The anonymization step in PRAM is performed by a record-wise fashion so anonymizing data in parallel is easy, and we can extend PRAM to a local perturbation, i.e., an individual anonymizes his/her data before sending them to the central server. In addition, PRAM does not need generalization, so we can obtain anonymized data with fine granularity and perform a fine-grained analysis on them. Furthermore, it is known that PRAM can satisfy ϵ -DP [12].

Although PRAM has these features and was proposed [9] before when the methods satisfying k -anonymization [20] and satisfying ϵ -DP [6] were proposed, it has been studied less than other approaches in the area of PPDP. Most popular methods for PPDP are evaluated in the context of k -anonymity. However, PRAM is a probabilistic method, so it cannot be evaluated in the context of k -anonymity. This means that no one can compare PRAM with other methods for PPDP in the same measure.

From the above circumstances, our aim of the paper is twofold. First, we extend k -anonymity for probabilistic methods (not only PRAM) for merging k -anonymity and ϵ -DP. Second, we evaluate how strongly PRAM preserves privacy in the context of k -anonymity.

1.2 Contributions

Our contributions are the following two points.

Extending k -anonymity for Probabilistic Methods We propose Pk -anonymity, which has the following four advantages compared to current probabilistic k -anonymity notions.

1. It is formally defined and sufficient to prove that it is a rigorous extension of the original k -anonymity. Specifically, we prove that k -anonymity and Pk -anonymity are totally equivalent if an anonymization algorithm is deterministic, in other words, if the algorithm is in the extent of conventional k -anonymization. We claim that one can consider a set of microdata anonymized using a probabilistic algorithm as k -anonymous if it is Pk -anonymous.

2. Its semantics is “no one estimates which person the record came from with more than $1/k$ probability (regardless of the link’s actual correctness).” From the viewpoint that privacy breaches are not only derived from correct information, this semantics is stronger than the prevention of only correct links.

3. Pk -anonymity never causes failure of anonymization. Some current probabilistic k -anonymity notions are defined as “satisfaction of k -anonymity with certain probability.” Unlike these notions, Pk -anonymity always casts a definite level of re-identification hardness to the adversary while it is defined via the theory of probability.

4. It is non-parametric; that is, no assumption on the distribution of raw microdata is necessary. Furthermore, it does not require any raw microdata to evaluate k .

Applying Pk -anonymity to PRAM Pk -anonymity on PRAM is analyzed. The value of k is derived from parameters of PRAM with no parametric assumption. Furthermore, we propose an algorithm to satisfy both Pk -anonymity (and ϵ -DP) with any value of k (and ϵ) is given.

1.3 Related Work

On Probabilistic k -anonymity Notions There are many studies on k -anonymity, and it has many supplemental privacy notions such as ℓ -diversity and t -closeness [10].

There have also been several studies that are relevant to the probability.

Wong et al. proposed (α, k) -anonymity [21]. Roughly speaking, (α, k) -anonymity states that (the original) k -anonymity is satisfied with probability α . Lodha and Thomas proposed $(1 - \beta, k)$ -anonymity. This is a relaxation from k -anonymity in a sample to that in a population. These two notions are essentially based on the original k -anonymity and are relaxations that allow failures of anonymization in a certain probability. Pk -anonymity is fully probabilistically defined and never causes failure of anonymization.

Aggarwal proposed a probabilistic k -anonymity [1]. Their goal was the same as with Pk -anonymity; however, it requires a parametric assumption that the distribution of raw microdata is a parallel translation of randomized microdata, and this seems to be rarely satisfied since a randomized distribution is generally flatter than the prior distribution.

Soria-Comas and Domingo-Ferrer also proposed their probabilistic k -anonymity [19]. They applied it to random swapping and micro-aggregation. The semantics of their anonymity is “no one can *correctly link* a person to a record with a higher probability than $1/k$ ” and Pk -anonymity is stronger. Unfortunately, further comparison is difficult since we could not find a sufficiently formal version of the definition.

On Privacy Measures Applicable to PRAM Aggarwal and Agrawal proposed a privacy measure based on conditional differential entropy [2]. This measure requires both raw and randomized data to be evaluated, unlike Pk -anonymity.

Agrawal et al. proposed (s, ρ_1, ρ_2) Privacy Breach [3], which is based on probability and applicable to retention-replacement perturbation. In contrast to k -anonymity, it does not take into account background knowledge concerning raw data, that is, concerning quasi-identifier attributes.

Rebollo-Monedero et al. [16] proposed a t -closeness-like privacy criterion and a distortion criterion which are applicable to randomization, and showed that PRAM can meet these criteria. Their work was aimed at clarifying the privacy-distortion trade-off problem via information theory, in the area of attribute estimation. Therefore, they did not mention whether PRAM can satisfy a well known privacy notion such as k -anonymity.

On Microdata Release Algorithms Satisfying k -anonymity and DP Li et al. proposed a method satisfying k -anonymity and (ϵ, δ) -DPS by combining random sampling and k -anonymization [11]. Since (ϵ, δ) -DPS is based on (ϵ, δ) -DP, PRAM’s ϵ -DP is stronger.

Soria-Comas and Domingo-Ferrer proposed methods for t -closeness and ϵ -DP. However, a certain amount of the adversary’s knowledge is assumed. Additionally, it cannot be applied when the adversary has any knowledge about all attributes. On the other hand, PRAM guarantees ϵ -DP regardless of the adversary’s knowledge.

On Probabilistic Anonymization Algorithms Related to PRAM There have been several studies [14, 17, 7, 4] on local perturbation in which individuals anonymize their respective data before transferring it to some central server.

Agrawal et al. proposed a FRAPP [4]. They use a specific transition probability matrix called MASK [17] and Cut and paste [8] to satisfy ρ_1 -to- ρ_2 privacy breach [7]. After that, Rastogi et al. [15] proposed the $\alpha\beta$ -algorithm that improves utility. These methods are closely related to PRAM, but they do not consider whether PRAM can satisfy a well-known notion such as k -anonymity.

1.4 Organization of Paper

In Section 2, we discuss the notations used in the paper and preliminary definitions. In Section 3, we propose our probabilistic k -anonymity, Pk -anonymity. In Section 4, we apply Pk -anonymity to PRAM and give algorithms for PRAM to satisfy both ϵ -DP and Pk -anonymity. In Section 5, we describe the experimental results regarding the utility of PRAM with parameters derived from the algorithms given in the previous sections. Finally, we state the conclusions of this paper in Section 6.

2 Preliminaries

2.1 Basic Settings

We consider two scenarios of microdata release using randomization. One is the setting in which a database administrator randomizes microdata (Figure 1(a)). The other is that in which individuals randomize their own records (Figure 1(b)). The latter is better with respect to privacy. PRAM is not only applicable to the former but also applicable to the latter [3] in contrast, k -anonymity can only be applied to the former. Thus, our Pk -anonymity is applicable to both scenarios via PRAM.

Since a person randomizes his/her data in the latter scenario, no one has all the raw microdata. Therefore, a person should be able to conduct appropriate randomization without another person's record. Fortunately, we can show that PRAM's parameter satisfying Pk -anonymity and DP can be determined using only the expected record count and metadata of attributes, as mentioned in Section 4.

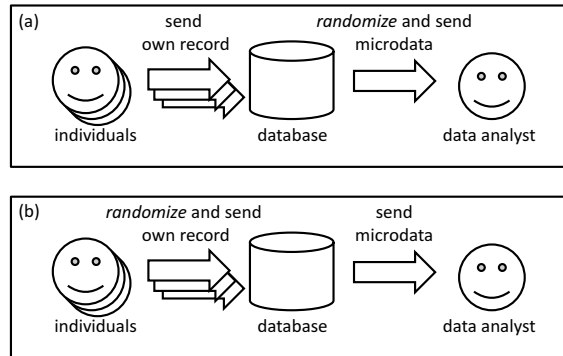


Fig. 1. Two Scenarios of Microdata Release using PRAM

2.2 Notation

We treat a table-formed database as both private and released data. Since the record count is revealed at the same time that the data are released in an ordinary microdata release, we assume that the record count is public and static in theory. Furthermore, we consider attributes as one bundled direct product attribute since it is sufficient for theoretical discussion.

Basically, we use the following notations.

- \mathcal{T} : the set of any private tables
- τ, T : a private table as an instance/random variable
- \mathcal{T}' : the set of any released tables
- τ', T' : a released table as an instance/random variable

- $\mathcal{R}, \mathcal{R}'$: the sets of all records in a private/released table
- $\mathcal{V}, \mathcal{V}'$: the sets of any values in a private/released table
- A : a transition probability matrix in PRAM
- f_X : the probability function of X where X is a random variable

In the discussion of multi-attributes, we also use the following notations.

- $\mathcal{A}, \mathcal{A}'$: the sets of attributes in a private/released table
- $\mathcal{V}_a, \mathcal{V}'_{a'}$ where $a \in \mathcal{A}$ and $a' \in \mathcal{A}'$: the sets of values in a private/released table, i.e., $\mathcal{V} = \prod_{a \in \mathcal{A}} \mathcal{V}_a$ and $\mathcal{V}' = \prod_{a' \in \mathcal{A}'} \mathcal{V}'_{a'}$ hold where \prod means the direct product.
- A_a where $a \in \mathcal{A}$: transition probability matrix of each attribute

We consider a table $\tau \in \mathcal{T}$ (or, $\tau' \in \mathcal{T}'$) as a map from \mathcal{R} to \mathcal{V} (or, \mathcal{R}' to \mathcal{V}'). More formally, we define τ (or, τ') as follows.

Definition 1. (*tables*)

Let a record set \mathcal{R} and a value set \mathcal{V} be finite sets. Then, the following map τ is called a table on $(\mathcal{R}, \mathcal{V})$.

$$\tau : \mathcal{R} \rightarrow \mathcal{V},$$

When we discuss a multi-attribute table, \mathcal{V} is represented as $\prod_{a \in \mathcal{A}} \mathcal{V}_a$, where an attribute set \mathcal{A} is a finite set, each \mathcal{V}_a is also a finite set for any $a \in \mathcal{A}$, and \prod means the direct product.

2.3 PRAM

PRAM [9] was proposed by Kooiman et al. in 1997 as a privacy preserving method for microdata release. It changes data according to a *transition probability matrix*. A transition probability matrix consists of probabilities in which each value in a private table will be changed into other specific (or the same) values. $A_{u,v}$ denotes the probability $u \in \mathcal{V}$ is changed into $v \in \mathcal{V}'$. For example, $A_{\text{male}, \text{female}}$ means “male \rightarrow female” is 25%.

PRAM is a quite general method. Invariant PRAM [9], retention-replacement perturbation [3], etc., are known as instantiations of it. Specifically, retention-replacement perturbation is simple and convenient.

Retention-replacement Perturbation In retention-replacement perturbation, individuals probabilistically replace their data with random data using given *retention probability* ρ . First, data are retained with ρ , and if the data are not retained, they will be replaced with a uniformly random value chosen from the attribute domain. Note that even if data are not retained, there is still the possibility that the data will not be changed, because the data value is included in the attribute domain as well as other values. For example, for an attribute “sex,” when $\rho = 0.5$, “male” is retained with $1/2$ probability, and with the remaining $1/2$ probability, it is replaced with a uniformly random value, namely, a value “female” and a value “male,” which is the same as the original, both with $1/2 \times 1/2 = 1/4$ probability. Eventually, the probability that “male” changes into “female” is $1/4$, and the probability that it does not change is $3/4$. The lower the retention probability, the higher privacy is preserved. On the contrary, the lower the probability, the lower utility. These probabilities form the following transition probability matrix.

$$\begin{bmatrix} 0.75 & 0.25 \\ 0.25 & 0.75 \end{bmatrix}$$

Generally, the transition probability matrix A_a of an attribute a is written as

$$(A_a)_{v_a, v'_a} = \begin{cases} \rho_a + \frac{(1 - \rho_a)}{|\mathcal{V}_a|} & \text{if } v_a = v'_a \\ \frac{(1 - \rho_a)}{|\mathcal{V}_a|} & \text{otherwise} \end{cases}$$

where for any $v \in \mathcal{V}$ and $a \in \mathcal{A}$, $v_a \in \mathcal{V}_a$ is an element of $v \in \mathcal{V}$ corresponding to a , and ρ_a is the retention probability corresponding to a .

2.4 k -anonymity

The k -anonymity [18] [20] is a privacy notion that is applicable to table-formed databases and defined as “for all database records, there are at least k records whose values are the same,” in other words, “no one can narrow down a person’s record to less than k records.”

Using the notations in Section 2.2, we represent the definition of k -anonymity [20] as follows.

Definition 2. (*k -anonymity*)

For a positive integer k , a released table $\tau' \in \mathcal{T}'$ is said to satisfy k -anonymity (or to be k -anonymous), if and only if it satisfies the following condition.

For any $r' \in \mathcal{R}'$, there are k or more \hat{r}' ’s such that $\hat{r}' \in \mathcal{R}'$ and $\tau'(r') = \tau'(\hat{r}')$.

A released table τ' in the above definition represents all columns corresponding to quasi-identifier attributes of an anonymized table.

However, the definition in [20] is problematic; i.e., there are some tables that satisfy k -anonymity but do not achieve its aim. For example, a table generated by copying all a private table’s records k times satisfies k -anonymity but it is obviously not safe. Therefore, we assume $|\mathcal{R}| = |\mathcal{R}'|$ to strengthen the above definition in the discussion of k -anonymity in this paper.

2.5 Anonymization and Privacy Mechanisms

We define anonymization and privacy mechanisms separately to discuss them formally. First we define anonymization.

Definition 3. (*anonymization*)

Let \mathcal{R} , \mathcal{R}' , \mathcal{V} and \mathcal{V}' be finite sets, \mathcal{T} and \mathcal{T}' be the sets of all tables on $(\mathcal{R}, \mathcal{V})$ and $(\mathcal{R}', \mathcal{V}')$, respectively, and let π be a map $\pi : \mathcal{R} \rightarrow \mathcal{R}'$. Then, for any $\tau \in \mathcal{T}$ and $\tau' \in \mathcal{T}'$, a map $\delta : \mathcal{T} \rightarrow (\mathcal{R} \rightarrow \mathcal{V}')$ is called anonymization with π from τ to τ' if and only if they satisfy

$$\delta(\tau) = \tau' \circ \pi, \quad (1)$$

where the notation $\mathcal{X} \rightarrow \mathcal{Y}$ denotes the set of all maps from \mathcal{X} to \mathcal{Y} for any set \mathcal{X} and \mathcal{Y} .

Anonymization δ represents an anonymization algorithm such as perturbation, k -anonymization, etc. A map π represents an anonymous communication channel, the shuffling function, or another component which hides the order of records in τ . In this paper, we adopt the uniformly random permutation as π .¹

Privacy mechanisms involve not only δ but also π , \mathcal{R} , \mathcal{R}' , \mathcal{V} and \mathcal{V}' , and random variables are brought to extend the above definitions to probabilistic ones. Random variables corresponding to τ , τ' , π , and δ are denoted by T , T' , Π , and Δ , respectively. We assume T , Π , and Δ are mutually independent as probabilistic events, while T' is dependent on the other three random variables.

Definition 4. (*privacy mechanisms*)

Let \mathcal{R} , \mathcal{R}' , \mathcal{V} , \mathcal{V}' , \mathcal{T} , and \mathcal{T}' be the same as Definition 3, and let T , T' , Π , and Δ be random variables on \mathcal{T} , \mathcal{T}' , $\mathcal{R} \rightarrow \mathcal{R}'$, and $\mathcal{T} \rightarrow (\mathcal{R} \rightarrow \mathcal{V}')$, respectively, such that T , Π , and Δ are mutually independent as probabilistic events, where the notation $\mathcal{X} \rightarrow \mathcal{Y}$ denotes the set of all maps from \mathcal{X} to \mathcal{Y} for any set \mathcal{X} and \mathcal{Y} . Then, the 6-tuple $(\mathcal{R}, \mathcal{V}, \mathcal{R}', \mathcal{V}', \Pi, \Delta)$ is called a privacy mechanism from T to T' if and only if they satisfy the following equation.

$$\Delta(T) = T' \circ \Pi$$

¹ A map π is essential for anonymization. For example, if the first record in the private table is to be the first record in the released table, identification is trivial.

2.6 Differential Privacy on PRAM

Dwork proposed DP [6] in 2006. It results in “an (statistical) output not changing much even if a database is changed with respect to at most one person.” Since it can be satisfied regardless of adversaries, it is being widely studied.

Differential privacy is defined with a real number parameter ε .

Definition 5. (ε -DP)

Let \mathcal{D} be a set of databases and d be a non-negative integer. A privacy mechanism $\mathcal{K} : \mathcal{D} \rightarrow \mathbb{R}^d$ is a probabilistic algorithm, and ε is a (small) positive real number. We say \mathcal{K} gives ε -DP if, and only if for $S \subseteq \text{Range}(\mathcal{K})$ and any pair D_1, D_2 of databases “differing at most by 1 element,” the following condition is satisfied.

$$\Pr[\mathcal{K}(D_1) \in S] \leq \exp(\varepsilon) \Pr[\mathcal{K}(D_2) \in S] \quad (2)$$

Note that what ‘databases’ and “differing at most by 1 element” mean remains free to interpretation.

Differential privacy is used as a privacy notion on interactive statistical databases as usual. However, PRAM is known to satisfy ε -DP for the query “`select * from τ` ” in SQL manner [12]. The query obviously represents the release of microdata. We introduce the known result [12] and discuss ε -DP on PRAM in addition to Pk -anonymity.

PRAM satisfies ε -DP with the following parameters [12].

Theorem 1. *For any PRAM mechanism Δ whose transition probability matrix is denoted by A , Δ gives ε -DP with the following ε .*

$$\varepsilon = \ln \max_{\substack{u, v \in \mathcal{V} \\ v' \in \mathcal{V}'}} \frac{A_{u, v'}}{A_{v, v'}}$$

The theorem has been already shown but it may not be rigorous and suit our notations. Therefore, we give another proof of Theorem 1 in Appendix A. We show a multi-attribute representation of Theorem 1 below. Simply, ε becomes the summation of each attribute’s ε .

Corollary 1. *For any PRAM mechanism Δ whose transition probability matrices are A_a for each attribute $a \in \mathcal{A}$, Δ gives ε -DP with the following ε .*

$$\varepsilon = \sum_{a \in \mathcal{A}} \ln \max_{\substack{u, v \in \mathcal{V}_a \\ v' \in \mathcal{V}'_a}} \frac{(A_a)_{u, v'}}{(A_a)_{v, v'}}$$

Regarding retention-replacement perturbation, ε is evaluated as follows.

Corollary 2. *For any retention-replacement perturbation Δ whose retention probabilities of each attribute are ρ_a , Δ gives ε -DP privacy with the following ε .*

$$\varepsilon = \sum_{a \in \mathcal{A}} \ln \frac{1 + (|\mathcal{V}_a| - 1)\rho_a}{1 - \rho_a} \quad (3)$$

3 Pk -anonymity

As the name suggests, k -anonymity represents anonymity among privacy notions. It is known that satisfying only anonymity is not enough to preserve privacy [13]; thus, further privacy notions that prevent attribute estimation were developed after k -anonymity. However, this *never* means that “anonymity is unnecessary.” These stronger privacy notions rely on the assumption that k -anonymity has already been satisfied. Therefore, the same as with deterministic microdata release, we consider anonymity as the first privacy requirement in randomization-based microdata release. Regarding randomization, however, anonymity has not yet been clarified. Obviously, this is a critical problem and should be solved as soon as possible.

3.1 Problem with k -anonymity on Randomization

We now explain what occurs when one applies k -anonymity directly to a randomized table. Imagine that one randomizes all records' quasi-identifiers uniformly randomly. Furthermore, suppose that the resulting table happens to have a record whose data are unique. The randomized table does not satisfy k -anonymity because it has a unique record. However, an adversary cannot identify anyone's record (without knowledge of sensitive attributes) since uniformly random values provide no information. In other words, the table should be considered as fully anonymous, although the table does not satisfy k -anonymity. Therefore, we need a new definition of k -anonymity applicable to randomization.

3.2 Intuitive Requirement

To apply k -anonymity to randomization, we have to determine what kind of notion we should construct. Intuitively, "no one can choose the correct record of a person with probability $1/k$ " is the likely choice. However, we have to take into account an adversary's incorrect presumption. Regarding privacy, the problem is not only the leakage of correct information, but the creation of *incorrect* information about a person. Since a person does not wish to reveal correct private information, neither the person nor the administrator of the database can resolve the adversary's misconception. Therefore, we require a stronger sentence, "no one *estimates* which person the record came from with more than $1/k$ probability." Note that this second sentence involves the first sentence (no one can choose...), because an adversary who correctly chooses the record of a person with probability $1/k$ is able to estimate the record at confidence $1/k$.

3.3 Background Knowledge of Adversary

In the definition of k -anonymity, there is no adversary, and this definition is described as a simple condition to be satisfied in a table. This is convenient for measuring k -anonymity. At the same time, however, it makes the meaning of privacy unclear.

Therefore, there is an adversary in our model of Pk -anonymity. The probability of linkage is varied according to the background knowledge of the adversary. In the Pk -anonymity model, an adversary's background knowledge is represented as a probabilistic function f_T^2 on the private table. Pk -anonymity requires the privacy mechanism of that the probability of linkage is bounded by $1/k$ for *all* f_T . It means that we deal with an adversary who has arbitrary knowledge about the private table: The adversary might know the private table itself and incorrect private tables.

We note that even if in the extreme case where the adversary knows the private table itself, Pk -anonymity can be satisfied by using the randomness in the privacy mechanisms. Of course, we assume that the adversary knows the released table, the anonymization algorithm, and parameters used in the system in addition to the background knowledge.

3.4 Definition of Pk -anonymity

We define our new anonymity, Pk -anonymity and Pk -anonymization, which is a privacy mechanism that always satisfies Pk -anonymity.

First, we define an attack by an adversary with background knowledge, which is represented as an estimation by the following probability, where τ' is a released table, Π is a uniformly random injective map from \mathcal{R} to \mathcal{R}' , $r \in \mathcal{R}$, $r' \in \mathcal{R}'$ and $\Delta(T) = T' \circ \Pi$.

$$\Pr[\Pi(r) = r' | T' = \tau'] \quad (4)$$

The term \mathcal{R} represents a set of individuals, and \mathcal{R}' represents a set of record IDs (not necessarily explicit IDs. In anonymized microdata, it maybe just a location in storage.). The Π 's randomness represents that

² It means that the adversary knows that the private table is τ_1 with probability x_1 , τ_2 with x_2 and so on. It is not a distribution of values in a specific table, but the distribution on the space of all tables.

“an adversary has no knowledge of the linkage between individuals and the records in τ' .” Taken together, the above probability represents the following probability from the standpoint of an adversary who saw τ' .

$$\Pr[\text{a person } r \text{'s record in } \tau' \text{ is } r']$$

We denote the above probability as $\mathcal{E}(f_T, \tau', r, r')$.

Next, we define Pk -anonymity.

Definition 6. (*Pk-anonymity*)

Let \mathcal{R} , \mathcal{V} , \mathcal{R}' , and \mathcal{V}' be finite sets, and Π and Δ be random variables on $\mathcal{R} \rightarrow \mathcal{R}'$ and $\mathcal{T} \rightarrow (\mathcal{R} \rightarrow \mathcal{V}')$, respectively, where \mathcal{T} denotes the set of tables on $(\mathcal{R}, \mathcal{V})$ and the notation $\mathcal{X} \rightarrow \mathcal{Y}$ denotes the set of all maps from \mathcal{X} to \mathcal{Y} for any set \mathcal{X} and \mathcal{Y} . Furthermore, let $\tilde{\Delta}$ denote a 6-tuple $(\mathcal{R}, \mathcal{V}, \mathcal{R}', \mathcal{V}', \Pi, \Delta)$.

Then, for any real number $k \geq 1$ and a table τ' on $(\mathcal{R}', \mathcal{V}')$, a pair $(\tilde{\Delta}, \tau')$ is said to satisfy Pk -anonymity (or to be Pk -anonymous) if and only if for any random variables T of tables on $(\mathcal{R}, \mathcal{V})$ and T' of tables on $(\mathcal{R}', \mathcal{V}')$ such that $\tilde{\Delta}$ is a privacy mechanism from T to T' , any record $r \in \mathcal{R}$ of the private table T and any record $r' \in \mathcal{R}'$ of the released table τ' , the following equation is satisfied.

$$\Pr[\Pi(r) = r' | T' = \tau'] \leq \frac{1}{k}$$

Definition 7. (*Pk-anonymization algorithms*)

Let \mathcal{R} , \mathcal{V} , \mathcal{R}' , \mathcal{V}' , Π , Δ , and $\tilde{\Delta}$ be the same as Definition 6, and let \mathcal{T}' denote the set of all tables on $(\mathcal{R}', \mathcal{V}')$.

Then, for any real number $k \geq 1$, $\tilde{\Delta}$ is said to be a Pk -anonymization if and only if $(\tilde{\Delta}, \tau')$ satisfies Pk -anonymity for any released table $\tau' \in \mathcal{T}'$ such that there exists a private table τ on $(\mathcal{R}, \mathcal{V})$ which satisfies $\Pr[\Delta(\tau) = \tau' \circ \Pi] \neq 0$.

we treat only Δ within 6-tuple of a privacy mechanism $(\mathcal{R}, \mathcal{V}, \mathcal{R}', \mathcal{V}', \Pi, \Delta) = \tilde{\Delta}$; thus, we do not differentiate $\tilde{\Delta}$ and Δ .

Pk -anonymity's direct meaning is “no one estimates which person the record came from with more than $1/k$ probability.” Intuitively, it seems to be similar to “no one can narrow down a person's record to less than k records,” which is an intuitive concept of k -anonymity. This intuitive similarity can also be confirmed mathematically. Furthermore, as far as deterministic anonymization algorithms, such as k -anonymization algorithms, are concerned, two anonymity notions can be shown to be equivalent to each other. Therefore, we say k -anonymity is satisfied in a randomized table if Pk -anonymity is satisfied in the table.

Theorem 2. For any positive integer k , privacy mechanism Δ , and released table τ' , the following relation holds if Δ is deterministic, i.e., for any $\tau \in \mathcal{T}$, there exists unique anonymized table $\hat{\tau}$ and $\Delta(\tau) = \hat{\tau}$.

$$\tau' \text{ is } k\text{-anonymous} \Leftrightarrow (\Delta, \tau') \text{ is } Pk\text{-anonymous}$$

This theorem represents equality of Pk -anonymity and k -anonymity under the consideration of deterministic anonymization algorithms, which are the applicable field of k -anonymity. Therefore, Pk -anonymity is deemed as an extension of k -anonymity.

(Proof of Theorem 2)

This theorem is shown with the following two lemmas.

Lemma 1. For any positive integer k , if a released table τ' is k -anonymous, then (Δ, τ') is Pk -anonymous for any privacy mechanism Δ .

Lemma 2. For any real number $t \geq 1$, positive number k such that $k \leq t$, any deterministic privacy mechanism Δ , and released table τ' , if (Δ, τ') is Pt -anonymous, then τ' is k -anonymous.

Roughly, Lemma 1 states that “ $k \Rightarrow Pk$ always,” and Lemma 2 states that “ $Pk \Rightarrow k$ if an anonymization algorithm is deterministic.”

(*Proof of Lemma 1*)

First, we use notation $\sharp_{\tau'}(v')$ as $|\tau'^{-1}(\{v'\})|$, and say r' is k -anonymous in τ' if $\sharp_{\tau'}(\tau'(r')) \geq k$. Then, k -anonymity of τ' is represented as “ r' is k -anonymous in τ' for any $r' \in \mathcal{R}'$.”

As mentioned in Section 3, we show Lemma 1 and Lemma 2. Note that the following equality holds by definition.

$$\Delta(T) = T' \circ \Pi \quad (5)$$

We show that an estimation probability, $\mathcal{E}(f_T, \tau', r, r')$, is equal to or less than $1/k$. For any background knowledge $f_T : \mathcal{T} \rightarrow \mathbb{R}$, any $r \in \mathcal{R}$ and any $r' \in \mathcal{R}'$, the following equations hold.

$$\begin{aligned} \mathcal{E}(f_T, \tau', r, r') &= \Pr[\Pi(r) = r' | T' = \tau'] \\ &= \frac{\Pr[\Pi(r) = r' \wedge T' = \tau']}{\Pr[T' = \tau']} = \frac{\Pr[\Pi(r) = r' \wedge \Delta(T) = \tau' \circ \Pi]}{\Pr[\Delta(T) = \tau' \circ \Pi]} \end{aligned} \quad (\text{from Equation (5)})$$

$$= \frac{\sum_{\substack{\delta: \mathcal{T} \rightarrow (\mathcal{R} \rightarrow \mathcal{V}') \\ \tau \in \mathcal{T}}} f_{\Delta}(\delta) f_T(\tau) \Pr[\Pi(r) = r' \wedge \delta(\tau) = \tau' \circ \Pi]}{\sum_{\substack{\delta: \mathcal{T} \rightarrow (\mathcal{R} \rightarrow \mathcal{V}') \\ \tau \in \mathcal{T}}} f_{\Delta}(\delta) f_T(\tau) \Pr[\delta(\tau) = \tau' \circ \Pi]}$$

(since T, Δ , and Π are independent of each other)

We define two propositions $\Phi(\delta, \tau)$ and $\hat{\Phi}(\delta, \tau)$ as

$$\Phi(\delta, \tau) = [\text{There exists } \hat{\pi} : \mathcal{R} \rightarrow \mathcal{R}' \text{ such that } \delta(\tau) = \tau' \circ \hat{\pi}]$$

$$\hat{\Phi}(\delta, \tau) = [\Phi(\delta, \tau) \text{ and } (\delta(\tau))(r) = \tau'(r')]$$

respectively. Since Π is a uniformly random permutation, the following equations hold.

$$\Pr[\delta(\tau) = \tau' \circ \Pi] = \begin{cases} \frac{\prod_{v' \in \text{Im}(\tau')} \sharp_{\tau'}(v')!}{|\mathcal{R}|!} & (\text{if } \Phi \text{ holds}) \\ 0 & (\text{otherwise}) \end{cases}$$

$$\Pr[\Pi(r) = r' \wedge \delta(\tau) = \tau' \circ \Pi]$$

$$\begin{aligned} &= \begin{cases} \frac{(\sharp_{\tau'}(\tau'(r')) - 1)! \prod_{v' \in \text{Im}(\tau') \setminus \{\tau'(r')\}} \sharp_{\tau'}(v')!}{|\mathcal{R}|!} & (\text{if } \hat{\Phi} \text{ holds}) \\ 0 & (\text{otherwise}) \end{cases} \\ &= \begin{cases} \frac{\prod_{v' \in \text{Im}(\tau')} \sharp_{\tau'}(v')!}{\sharp_{\tau'}(\tau'(r')) |\mathcal{R}|!} & (\text{if } \hat{\Phi} \text{ holds}) \\ 0 & (\text{otherwise}) \end{cases} \end{aligned}$$

Therefore, the primary equation $\Pr[\Pi(r) = r' | T' = \tau']$ is transformed as

$$\frac{\sum_{\hat{\Phi}(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(\tau'(s'))!}{\#_{\tau'}(\tau'(r')) |\mathcal{R}|!}}{\sum_{\Phi(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(\tau'(s'))!}{|\mathcal{R}|!}} \leq \frac{\sum_{\Phi(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(\tau'(s'))!}{\#_{\tau'}(\tau'(r')) |\mathcal{R}|!}}{\sum_{\Phi(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(\tau'(s'))!}{|\mathcal{R}|!}}$$

(since $\hat{\Phi} \Rightarrow \Phi$)

$$= \frac{1}{\#_{\tau'}(\tau'(r'))} \leq \frac{1}{k}.$$

(from k -anonymity)

□(Lemma 1)

(Proof of Lemma 2)

In the proof we use and show the following contraposition.

For any privacy mechanism Δ , if τ' is not k -anonymous, then (Δ, τ') is also not Pt -anonymous.

We consider the background knowledge, f_T , satisfying $f_T(\tau) = 1$. Let $r' \in \mathcal{R}'$ be a record that is not k -anonymous in τ' and that satisfies $r \in \pi^{-1}(r')$.

As in the proof of Lemma 1, the following equation holds.

$$\mathcal{E}(f_T, \tau', r, r') = \frac{\sum_{\hat{\Phi}(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{\#_{\tau'}(\tau'(r')) |\mathcal{R}|!}}{\sum_{\Phi(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{|\mathcal{R}|!}}$$

Since Δ is deterministic and $f_T(\tau) = 1$, we transform the above equation as follows.

$$\frac{\sum_{\hat{\Phi}(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{\#_{\tau'}(\tau'(r')) |\mathcal{R}|!}}{\sum_{\Phi(\delta, \tau)} f_{\Delta}(\delta) f_T(\tau) \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{|\mathcal{R}|!}} = \frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{\frac{\prod_{v' \in \text{Im}(\tau')} \#_{\tau'}(v')!}{\#_{\tau'}(\tau'(r')) |\mathcal{R}|!}} = \frac{1}{\#_{\tau'}(\tau'(r'))}.$$

We assume r' is not k -anonymous; therefore, $\frac{1}{\#_{\tau'}(\tau'(r'))} \geq \frac{1}{k}$.

□(Lemma 2)

The above two lemmata immediately imply Theorem 2.

□

Furthermore, k -anonymization and Pk -anonymization also have a similar equality.

Corollary 3. *For any positive integer k and privacy mechanism Δ , if Δ is deterministic, the following holds.*

$$\Delta \text{ is } k\text{-anonymization} \Leftrightarrow \Delta \text{ is } Pk\text{-anonymization}$$

Through Theorem 2, we have seen that Pk -anonymity is an exact mathematical extension of k -anonymity. Moreover, the intuitive meaning of k -anonymity, “no one can narrow down a person’s record to less than k records” is applicable from the following viewpoint. Under a privacy mechanism Δ and a certain released table τ' , an adversary’s estimation $\mathcal{E}(f_T, \tau', r, r')$ is $1/k$ or less for any $r \in \mathcal{R}$ and $r' \in \mathcal{R}'$, when (Δ, k) is Pk -anonymous. Then by definition, for any $k - 1$ records $\{r'_i\}_{0 \leq i < k-1}$ in τ' , the following relation holds.

$$\sum_{0 \leq i < k-1} \mathcal{E}(f_T, \tau', r, r'_i) \leq 1 - \frac{1}{k} \preceq 1$$

This relation means that when one has chosen $k - 1$ records from τ' , there is always $1/k$ probability that r is not in these $k - 1$ records in τ' . This precisely means that “no one can narrow down a person’s record to less than k records.”

Remember that an adversary is considered as background knowledge and a distribution. In the field of cryptography, an adversary is often represented as an algorithm. We show that an adversary represented as a probabilistic algorithm M that takes inputs as (τ', r) cannot select r ’s record in a released table with a higher probability than $1/k$.

Proposition 1. *For any Pk -anonymization Δ , $\tau \in T$, $\tau' \in T'$ such that $\Delta(T) = T' \circ \Pi$, $r \in \mathcal{R}$ and probabilistic algorithm M that takes τ and r as inputs, M do not select $r' \in \mathcal{R}'$ such that $\Pi(r) = r'$ with a higher probability than $1/k$.*

(Proof of Proposition 1)

Let f_T be the following probability function.

$$\Pr[T = \tau] = \begin{cases} 1 & \text{if } \tau = \tau_t \\ 0 & \text{otherwise} \end{cases}$$

Under this f_T , the probability $\Pr[\Pi(r) = r' | T' = \tau']$ is not only an adversary’s estimate, but also the true probability. On the other hand, it is $1/k$ or smaller by Pk -anonymity; therefore, no function selects r' with a higher probability than $1/k$, and M is only a function.

□

4 Applying Pk -anonymity (and DP) to PRAM

We apply Pk -anonymity to PRAM. First, we show a theorem on general PRAM for calculating k . Next, we describe a more concrete formula on retention-replacement perturbation introduced in Section 2.3. Finally, combining existing result, we propose an algorithm to satisfy both Pk -anonymity and ε -DP.

We assume $\mathcal{V} = \mathcal{V}'$. The privacy mechanism Δ is defined along with PRAM, i.e., defined for any $r \in \mathcal{R}$ and $v' \in \mathcal{V}'$, as follows.

$$f_{(\Delta(T))(r)}(v') = A_{T(r), v'}$$

We call such a privacy mechanism a PRAM mechanism.

Theorem 3. (*Pk -anonymity on PRAM*)

A PRAM mechanism whose transition probability matrix is A is a Pk -anonymization if and only if k is described as follows.

$$k \leq 1 + (|\mathcal{R}| - 1) \min_{\substack{u, v \in \mathcal{V} \\ u', v' \in \mathcal{V}'}} \frac{A_{u, v'} A_{v, u'}}{A_{u, u'} A_{v, v'}}$$

Note that this theorem shows the tight bound of k . This theorem is shown by evaluating the maximum probability of estimation $\mathcal{E}(f_T, \tau', r, r')$ on $r \in \mathcal{R}, r' \in \mathcal{R}', \tau' \in \mathcal{T}'$ and background knowledge $f_T : \mathcal{T} \rightarrow \mathbb{R}$. The probability takes the maximum value in the following case.

- All values in private table τ happened to be retained in released table τ'
- There are only two values in τ and τ' , one is $\tau(r)$ and the other is $v \in \mathcal{V}$, which satisfies $\tau(s) = v$ for any record $s \neq r$
- $\tau(r)$ and v shown above are different from each other in all attributes
- The adversary knows all about the private table, i.e., $f_T(\tau) = \begin{cases} 1 & \text{if } \tau = \tau' \\ 0 & \text{otherwise} \end{cases}$

With this fact, k can be derived by substituting each parameter in estimate $\mathcal{E}(f_T, \tau', r, r')$.

(Proof of Theorem 3)

We show this theorem by evaluating the maximum of $\mathcal{E}(f_T, \tau', r, r')$ on $r \in \mathcal{R}, r' \in \mathcal{R}', \tau' \in \mathcal{T}'$ and $f_T : \mathcal{T} \rightarrow \mathbb{R}$. Similar to the proof of Lemma 1, the following equation holds.

$$\begin{aligned} \mathcal{E}(f_T, \tau', r, r') &= \Pr[\Pi(r) = r' | T' = \tau'] \\ &= \frac{\Pr[\Delta(T) = \tau' \circ \Pi \wedge \Pi(r) = r']}{\Pr[\Delta(T) = \tau' \circ \Pi]} \end{aligned} \tag{from Equation (5)}$$

$$= \frac{\sum_{\tau \in \mathcal{T}} f_T(\tau) \Pr[\Delta(\tau) = \tau' \circ \Pi \wedge \Pi(r) = r']}{\sum_{\tau \in \mathcal{T}} f_T(\tau) \Pr[\Delta(\tau) = \tau' \circ \Pi]}$$

Next we show that f_T maximizes the above estimation probability. In other words, we show which adversary can guess the record of a person with the highest confidence.

Lemma 3. *Let \mathbb{R}^{n+} be the set of non-zero n -dim vectors whose elements are non-negative real numbers. Then for any vector $a, b \in \mathbb{R}^{n+}$, the maximum of*

$$g(x) \stackrel{\text{def}}{=} \frac{b \cdot x}{a \cdot x} (= \frac{\sum_{i < n} b_i x_i}{\sum_{i < n} a_i x_i})$$

on a variable x on \mathbb{R}^{n+} is $\max_{i < n} \frac{b_i}{a_i}$, and x satisfies

$$\text{for any } i < n \text{ such that } \frac{b_i}{a_i} \neq \max_{i < n} \frac{b_i}{a_i}, x_i = 0.$$

(proof of Lemma 3)

Since $g(x)$ is invariant on a scalar multiplication of x , it is sufficient to find the maximum in some $Y \subset \mathbb{R}^{n+}$ such that there exist $\alpha \in \mathbb{R}$ and $y \in Y$ that satisfy $\alpha y = x$, for $x \in \mathbb{R}^{n+}$. By taking Y as a plane, we can find that the maximum exists because it is a bounded closed set.

Next we have that

$$x_i = 0 \text{ or } \frac{\partial g(x)}{\partial x_i} = 0$$

holds for each element x_i of $x \in \mathbb{R}^{n+}$ that gives maximum $g(x)$. Otherwise, escalating x_i should increase the value of $g(x)$, and contradicts that $g(x)$ is the maximum. Because of this fact and also because that x is not a zero vector, there must exist at least one i such that $\frac{\partial g(x)}{\partial x_i} = 0$.

Finally, this partial differential is found to be

$$\frac{\partial g(x)}{\partial x_i} = \frac{(a \cdot x)b_i - (b \cdot x)a_i}{(a \cdot x)^2},$$

then

$$\frac{\partial g(x)}{\partial x_i} = 0 \Leftrightarrow g(x) = \frac{b_i}{a_i}$$

holds. Therefore, i , which satisfies $\frac{\partial g(x)}{\partial x_i} = 0$ must be i giving maximum $\frac{b_i}{a_i}$; all other elements are 0, and the maximum of $g(x)$ is $\max_{i < n} \frac{b_i}{a_i}$.

□(Lemma 3)

From the above lemma, when $\mathcal{E}(f_T, \tau', r, r')$ takes the maximum, f_T makes the following formula maximum,

$$\frac{\Pr[\Delta(\tau) = \tau' \circ \Pi \wedge \Pi(r) = r']}{\Pr[\Delta(\tau) = \tau' \circ \Pi]} \quad (6)$$

and the maximum of Formula (6) is equal to that of $\mathcal{E}(f_T, \tau', r, r')$.

Since Π is a uniformly random permutation, Formula (6) is transformed as follows.

$$\begin{aligned} \text{Formula(6)} &= \frac{\frac{1}{|\mathcal{R}|!} \sum_{\pi(r)=r'} \Pr[\Delta(\tau) = \tau' \circ \pi]}{\frac{1}{|\mathcal{R}|!} \sum_{\pi} \Pr[\Delta(\tau) = \tau' \circ \pi]} \\ &= \frac{\sum_{\pi(r)=r'} \Pr[\Delta(\tau) = \tau' \circ \pi]}{\sum_{\pi} \Pr[\Delta(\tau) = \tau' \circ \pi]} = \frac{\sum_{\pi(r)=r'} \prod_{s \in \mathcal{R}} \Pr[(\Delta(\tau))(s) = \tau'(\pi(s))]}{\sum_{\pi} \prod_{s \in \mathcal{R}} \Pr[(\Delta(\tau))(s) = \tau'(\pi(s))]} \end{aligned}$$

(since Δ is independent from each record)

Let a matrix $A^{\tau, \tau'}$ be

$$A_{s, s'}^{\tau, \tau'} \stackrel{\text{def}}{=} \Pr[(\Delta(\tau))(s) = \tau'(s')]$$

for any $s \in \mathcal{R}, s' \in \mathcal{R}'$. Then, the above formula is represented as follows.

$$F(A^\tau) \stackrel{\text{def}}{=} \frac{\sum_{\pi(r)=r'} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}}{\sum_{\pi} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}}$$

We would rather find the minimum of the reciprocal than the maximum of $F(A^{\tau, \tau'})$ itself. In the case of $|\mathcal{R}| \geq 2$, the reciprocal is transformed as follows.

$$\frac{1}{F(A^{\tau, \tau'})} = \frac{\sum_{\pi} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}}{\sum_{\pi(r)=r'} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}}$$

$$\begin{aligned}
& \frac{\sum_{\substack{t \neq r \\ t' \neq r'}} A_{t,r'}^{\tau,\tau'} A_{r,t'}^{\tau,\tau'} \sum_{\substack{\pi(t)=r' \\ \pi(r)=t'}} \prod_{s \neq t,r} A_{s,\pi(s)}^{\tau,\tau'} + A_{r,r'}^{\tau,\tau'} \sum_{\pi(r)=r'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}}{A_{r,r'}^{\tau,\tau'} \sum_{\pi(r)=r'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}} \\
&= 1 + \frac{\sum_{\substack{t \neq r \\ t' \neq r'}} A_{t,r'}^{\tau,\tau'} A_{r,t'}^{\tau,\tau'} \sum_{\substack{\pi(t)=r' \\ \pi(r)=t'}} \prod_{s \neq t,r} A_{s,\pi(s)}^{\tau,\tau'}}{A_{r,r'}^{\tau,\tau'} \sum_{\pi(r)=r'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}} = 1 + \frac{\sum_{\substack{t \neq r \\ t' \neq r'}} A_{t,r'}^{\tau,\tau'} A_{r,t'}^{\tau,\tau'} \sum_{\substack{\pi(r)=r' \\ \pi(t)=t'}} \prod_{s \neq t,r} A_{s,\pi(s)}^{\tau,\tau'}}{A_{r,r'}^{\tau,\tau'} \sum_{\pi(r)=r'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}} \\
&= 1 + \frac{\sum_{t \neq r} A_{t,r'}^{\tau,\tau'} A_{r,\pi(t)}^{\tau,\tau'} \sum_{\pi(r)=r'} \frac{\prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}}{A_{t,\pi(t)}^{\tau,\tau'}}}{A_{r,r'}^{\tau,\tau'} \sum_{\pi(r)=r'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}} = 1 + \frac{\sum_{\pi(r)=r'} \sum_{t \neq r} \frac{A_{t,r'}^{\tau,\tau'} A_{r,\pi(t)}^{\tau,\tau'}}{A_{t,\pi(t)}^{\tau,\tau'}} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}}{\sum_{\pi(r)=r'} A_{r,r'}^{\tau,\tau'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}}
\end{aligned}$$

We show the following lemma.

Lemma 4. Let g_i and h_i be $g_i, h_i : \mathbb{R}^{\mathcal{I}} \rightarrow \mathbb{R}$ for any index $i \in \mathcal{I}$, where \mathcal{I} is a set of indices. If some $x \in \mathbb{R}^{\mathcal{I}}$ and $z \in \mathbb{R}$ satisfy $\frac{h_i(x)}{g_i(x)} = \min_{x' \in \mathbb{R}^{\mathcal{I}}} \frac{h_i(x')}{g_i(x')} = z$ for any $i \in \mathcal{I}$, then the following equation is satisfied.

$$\min_{x' \in \mathbb{R}^{\mathcal{I}}} \frac{\sum_{i \in \mathcal{I}} h_i(x')}{\sum_{i \in \mathcal{I}} g_i(x')} = \frac{\sum_{i \in \mathcal{I}} h_i(x)}{\sum_{i \in \mathcal{I}} g_i(x)}$$

(proof of Lemma 4)

From the assumption of the lemma, $h_i(x') \geq z g_i(x')$ hold for all $i \in \mathcal{I}$ and any $x' \in \mathbb{R}$. Therefore,

$$\frac{\sum_{i \in \mathcal{I}} h_i(x')}{\sum_{i \in \mathcal{I}} g_i(x')} \geq z,$$

then

$$\min_{x' \in \mathbb{R}^n} \frac{\sum_{i \in \mathcal{I}} h_i(x')}{\sum_{i \in \mathcal{I}} g_i(x')} = \frac{\sum_{i \in \mathcal{I}} h_i(x)}{\sum_{i \in \mathcal{I}} g_i(x)}$$

holds.

□(Lemma 4)

Let $h_{\pi}(A^{\tau,\tau'})$ and $g_{\pi}(A^{\tau,\tau'})$ be

$$\begin{aligned}
h_{\pi}(A^{\tau,\tau'}) &= \sum_{t \neq r} \frac{A_{t,r'}^{\tau,\tau'} A_{r,\pi(t)}^{\tau,\tau'}}{A_{t,\pi(t)}^{\tau,\tau'}} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}, \\
g_{\pi}(A^{\tau,\tau'}) &= A_{r,r'}^{\tau,\tau'} \prod_{s \neq r} A_{s,\pi(s)}^{\tau,\tau'}
\end{aligned}$$

for any $\pi : \mathcal{R} \rightarrow \mathcal{R}'$. Thanks to Lemma 4, it is sufficient to consider $\frac{h_\pi(A^{\tau, \tau'})}{g_\pi(A^{\tau, \tau'})}$ only. Because it is transformed into $\frac{1}{A_{r, r'}^{\tau, \tau'} \sum_{t \neq r} \frac{A_{t, r'}^{\tau, \tau'} A_{r, \pi(t)}^{\tau, \tau'}}{A_{t, \pi(t)}^{\tau, \tau'}}$, it takes the minimum for any $\pi : \mathcal{R} \rightarrow \mathcal{R}'$ when τ and τ' are as follows.

There exists $v \in \mathcal{V}$ and $v' \in \mathcal{V}'$ such that $\frac{A_{v, \tau'(r')} A_{\tau(r), v'}}{A_{\tau(r), \tau'(r')} A_{v, v'}} = \min_{\substack{u, v \in \mathcal{V} \\ u', v' \in \mathcal{V}'}} \frac{A_{u, v'} A_{v, u'}}{A_{u, u'} A_{v, v'}}$, $\tau(s) = v$ for any $s \neq r$ and $\tau'(s') = v'$ for any $s' \neq r'$.

Since k is to be the reciprocal of the maximum of $F(A^{\tau, \tau'})$, k is found to be the following value.

$$k = 1 + (|\mathcal{R}| - 1) \min_{\substack{u, v \in \mathcal{V} \\ u', v' \in \mathcal{V}'}} \frac{A_{u, v'} A_{v, u'}}{A_{u, u'} A_{v, v'}}$$

It is easy to confirm that the above equation also holds when $|\mathcal{R}| = 1$. In this case, since only one π exists (denoted as $\hat{\pi}$), k equals 1 as follows.

$$k = \frac{1}{F(A^{\tau, \tau'})} = \frac{\sum_{\pi} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}}{\sum_{\pi(r)=r'} \prod_{s \in \mathcal{R}} A_{s, \pi(s)}^{\tau, \tau'}} = \frac{\prod_{s \in \mathcal{R}} A_{s, \hat{\pi}(s)}^{\tau, \tau'}}{\prod_{s \in \mathcal{R}} A_{s, \hat{\pi}(s)}^{\tau, \tau'}} = 1 = 1 + (|\mathcal{R}| - 1) \min_{\substack{u, v \in \mathcal{V} \\ u', v' \in \mathcal{V}'}} \frac{A_{u, v'} A_{v, u'}}{A_{u, u'} A_{v, v'}} \quad (\text{since } |\mathcal{R}| = 1)$$

□

We describe the multi-attribute version of Theorem 3.

Corollary 4. *A PRAM mechanism whose transition probability matrices are A_a for each attribute a is a Pk -anonymization when k is described as follows,*

$$k = 1 + (|\mathcal{R}| - 1) \prod_{a \in \mathcal{A}} \text{AR}_a$$

where AR_a is

$$\text{AR}_a = \min_{\substack{u, v \in \mathcal{V} \\ u', v' \in \mathcal{V}'}} \frac{(A_a)_{u, v'} (A_a)_{v, u'}}{(A_a)_{u, u'} (A_a)_{v, v'}}.$$

The following corollary is applicable to retention-replacement perturbation.

Corollary 5. *Retention-replacement perturbation whose retention probabilities are ρ_a for each attribute $a \in \mathcal{A}$, is a Pk -anonymization when k is described as follows,*

$$k = 1 + (|\mathcal{R}| - 1) \prod_{a \in \mathcal{A}} \text{AR}_a$$

where AR_a is

$$\text{AR}_a = \left(\frac{1 - \rho_a}{1 + (|\mathcal{V}_a| - 1)\rho_a} \right)^2.$$

Using Theorem 3, k is easily calculated with the record count $|\mathcal{R}|$ and transition probability matrix A . Regarding retention-replacement perturbation, A is determined independently with the instance of private data, k is calculated with the record count $|\mathcal{R}|$ and the numbers of attribute values $|\mathcal{V}_a|$ and retention probabilities ρ_a only, for each attribute a .

Conversely, ρ_a are also calculated in retention-replacement perturbation. By letting all ρ_a be the same ρ over all attributes, the equation is transformed as follows.

$$k = 1 + (|\mathcal{R}| - 1) \left(\prod_{a \in \mathcal{A}} \frac{1 - \rho}{1 + (|\mathcal{V}_a| - 1)\rho} \right)^2 \quad (7)$$

Since k monotonically decreases on $0 \leq \rho \leq 1$, ρ is easily and uniquely solved using, for example, the bisection method for any k , $|\mathcal{R}|$ and $|\mathcal{V}_a|$ (Algorithm 1). Note that k is allowed to be a real number, for example, $k = 1.5$.

Algorithm 1 determining ρ in retention-replacement perturbation from k

input: $k \in \mathbb{R}(k \geq 1)$, $|\mathcal{R}| \in \mathbb{N}$, $|\mathcal{V}_a|$ for each attribute

output: retention probability ρ

1: Set $\rho_0 = 1/2$.

2: Run the bisection method with ρ 's initial value ρ_0 with respect to k using Equation (7) and output the converged ρ .

For example, to ensuring $P100$ -anonymity on 100,000 records of data, ρ is calculated as roughly 0.303, where there are three attributes, sex, age from 20's to 60's, and 10-leveled annual income.

When the record count is uncertain since the data are to be collected thereafter, it is sufficient to use the expected record count. Even when the record count does not reach the expected value, Pk -anonymity is still satisfied for the following reason. When each record in table τ' is anonymous due to an anonymous communication channel, it can be said that only a part of table τ' is visible in the state in which τ' is being collected. An estimation in such a situation is equivalent to that from the algorithm that ignores the absent records. From Proposition 1, the algorithm cannot derive $\mathcal{E}(f_T, \tau', r, r') \geq 1/k$ if it is correct.

4.1 DP on PRAM in Addition to Pk-Anonymity

Regarding retention-replacement perturbation, we can derive Algorithm 2 that determines the parameter in order to satisfy ε -DP from Corollary 2.

Algorithm 2 determining ρ from ε

input: $\varepsilon > 0$ and $|\mathcal{V}_a|$ for each attribute a

output: retention probability ρ

1: Set $\rho_0 = 1/2$.

2: Run the bisection method with ρ 's initial value ρ_0 with respect to ε using Equation (3), and output the converged ρ .

Combining Algorithm 2 with Algorithm 1, we have Algorithm 3 that determines the parameter in order to satisfy both Pk -anonymity and ε -DP.

5 Experimental results

From the aspect of utility, we show that randomized data-bases protected by Pk -anonymity are available for data analyses. We experimented with cross-tabulations (or, contingency tables) using Pk -anonymity.

In the experiments discussed below, the dataset was randomized by retention-replacement perturbation, and cross tabulations were calculated using the reconstruction method [3]. The target dataset was the US

Algorithm 3 determining ρ from k and ε

input: $k \in \mathbb{R}(k \geq 1)$, $\varepsilon > 0$, $|\mathcal{R}| \in \mathbb{N}$, $|\mathcal{V}_a|$ for each attribute

output: retention probability ρ

1: Run Algorithm 1 and Algorithm 2 and let the results be ρ_k and ρ_ε , respectively.

2: output $\min(\rho_k, \rho_\varepsilon)$.

census dataset in the UCI Machine Learning Repository [5], which has 2,458,285 records. Out of this dataset, we extracted and used 7 attributes, as shown on Table 1. Several attributes were rounded because they had too many attribute values for cross tabulation.

Table 1. attributes and number of attribute values

Sex	2
Age[*]	18
Total Pers. Inc. Signed[*]	12
Worked Last Yr. 1989	3
Worked Last Week	3
Ed. Attainment	18
Travel Time to Work[*]	20

(Marked([*]) attributes are rounded.)

Figure 2 shows $L1$ -norm errors and ϵ by varying the record count with fixed $k = 2$ and four attributes, Sex, Age, Total Pers. Inc. Signed, and Worked Last Yr. 1989. The $L1$ -norm is a normalized distance between original cross-tabulated aggregates and reconstructed aggregates, given as the following d , where each x_v and y_v are the counted aggregates of the private table and the reconstructed aggregates corresponding to $v \in \mathcal{V}$, respectively.

$$d = \frac{\sum_{v \in \mathcal{V}} |x_v - y_v|}{|\mathcal{R}|}$$

From the graph, it seems that errors become smaller as the record count increases. When only 245 records were used, errors were quite high. However, there were almost no errors when all 2,458,285 records were used. This is due to two reasons. First, in the reconstruction method, a large number of records generally results in accurate analyses results in a fixed retention probability. Second, since many records also provide high k on Pk -anonymity by the same ρ according to Theorem 3, one can set a relatively high ρ . Regarding ε -DP, ε increases as the record count increases. It is because retention probability ρ monotonically increases with the increase of the record count by Equation (7), when k is fixed;

Figure 3 shows $L1$ -norm errors and ϵ by varying the number of attributes with fixed $k = 2$, using all the records of the dataset. Attributes have been added in the same order as in Table 1. Figure 4 shows $L1$ -norm errors and ϵ by varying k with fixed attributes. All the records from the dataset were used and attributes were the same four attributes as in Figure 2. From these graphs, it seems that errors become larger as the number of attributes or k increases. However, the increment is quite small.

6 Conclusions

In the field of anonymized microdata release, we mainly presented the following two theories. We first proposed an anonymity notion, Pk -anonymity, which is an extension of k -anonymity to randomized microdata, and its intuitive meaning is “no one estimates which person the record came from with more than $1/k$

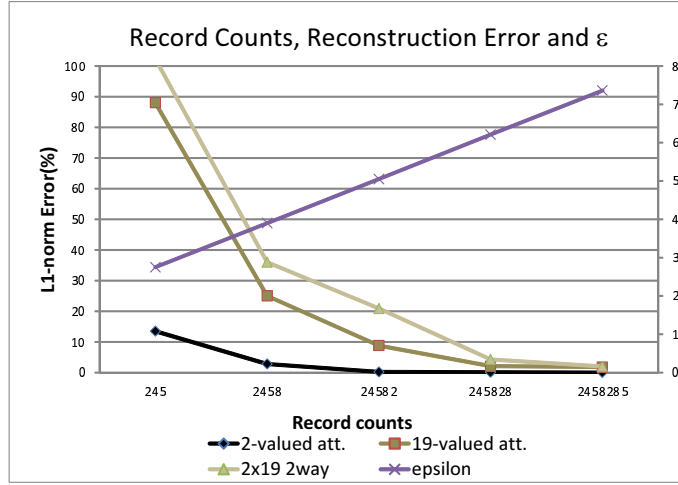


Fig. 2. Reconstruction errors and ϵ by varying number of records

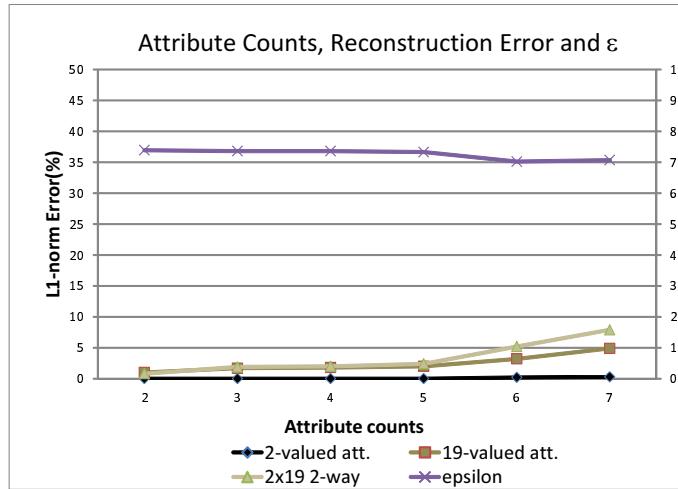


Fig. 3. Reconstruction errors and ϵ by varying number of attributes
p

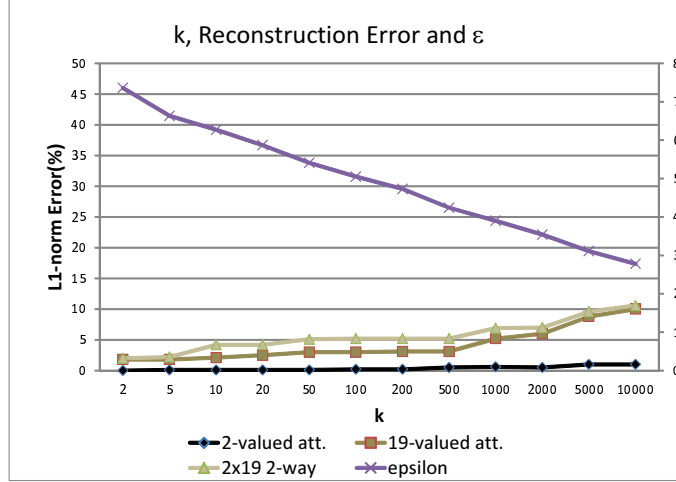


Fig. 4. Reconstruction errors and ϵ by varying k

probability.” We then applied Pk -anonymity to PRAM. PRAM is known to satisfy ϵ -DP; thus, it achieves k -anonymous and ϵ -differentially private microdata release.

The contributions of the paper are:

- an anonymity notion called Pk -anonymity,
- proofs that Pk -anonymity is an exact mathematical extension of k -anonymity,
- a formula for calculating k on PRAM,
- algorithms for determining the parameter of the retention-replacement perturbation according to k and ϵ ,
- experimental results to empirically analyze the trade-off relation between utility and privacy/anonymity using a real dataset.

Theoretical analyses and further experiments in real applications regarding utility are future work.

References

1. C. C. Aggarwal. On unifying privacy and uncertain data models. In G. Alonso, J. A. Blakeley, and A. L. P. Chen, editors, *ICDE*, pages 386–395. IEEE, 2008.
2. D. Agrawal and C. C. Aggarwal. On the design and quantification of privacy preserving data mining algorithms. In P. Buneman, editor, *PODS*. ACM, 2001.
3. R. Agrawal, R. Srikant, and D. Thomas. Privacy preserving olap. In F. Özcan, editor, *SIGMOD Conference*, pages 251–262. ACM, 2005.
4. S. Agrawal, J. R. Haritsa, and B. A. Prakash. FRAPP: a framework for high-accuracy privacy-preserving mining. *Data Min. Knowl. Discov.*, 18(1):101–139, 2009.
5. C. Blake and C. Merz. UCI repository of machine learning databases, 1998.
6. C. Dwork. Differential privacy. In M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, editors, *ICALP (2)*, volume 4052 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2006.
7. A. V. Evfimievski, J. Gehrke, and R. Srikant. Limiting privacy breaches in privacy preserving data mining. In F. Neven, C. Beeri, and T. Milo, editors, *Proceedings of the Twenty-Second ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems, June 9-12, 2003, San Diego, CA, USA*, pages 211–222. ACM, 2003.
8. A. V. Evfimievski, R. Srikant, R. Agrawal, and J. Gehrke. Privacy preserving mining of association rules. *Inf. Syst.*, 29(4):343–364, 2004.
9. P. Kooiman, L. Willenborg, and J. Gouweleeuws. PRAM: A method for disclosure limitation of microdata. *Research report no. 90*, 1997.

10. N. Li, T. Li, and S. Venkatasubramanian. t-closeness: Privacy beyond k-anonymity and l-diversity. In R. Chirkova, A. Dogac, M. T. Özsu, and T. K. Sellis, editors, *ICDE*, pages 106–115. IEEE, 2007.
11. N. Li, W. H. Qardaji, and D. Su. On sampling, anonymization, and differential privacy or, *k*-anonymization meets differential privacy. In H. Y. Youm and Y. Won, editors, *ASIACCS*, pages 32–33. ACM, 2012.
12. B.-R. Lin, Y. Wang, and S. Rane. A framework for privacy preserving statistical analysis on distributed databases. In *WIFS*, pages 61–66. IEEE, 2012.
13. A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkatasubramanian. l-diversity: Privacy beyond k-anonymity. In L. Liu, A. Reuter, K.-Y. Whang, and J. Zhang, editors, *ICDE*, page 24. IEEE Computer Society, 2006.
14. N. Mishra and M. Sandler. Privacy via pseudorandom sketches. In *Proceedings of the Twenty-fifth ACM SIGMOD-SIGACT-SIGART Symposium on Principles of Database Systems*, PODS ’06, pages 143–152, New York, NY, USA, 2006. ACM.
15. V. Rastogi, S. Hong, and D. Suciu. The boundary between privacy and utility in data publishing. In C. Koch, J. Gehrke, M. N. Garofalakis, D. Srivastava, K. Aberer, A. Deshpande, D. Florescu, C. Y. Chan, V. Ganti, C. Kanne, W. Klas, and E. J. Neuhold, editors, *Proceedings of the 33rd International Conference on Very Large Data Bases, University of Vienna, Austria, September 23-27, 2007*, pages 531–542. ACM, 2007.
16. D. Rebollo-Monedero, J. Forné, and J. Domingo-Ferrer. From t-closeness-like privacy to postrandomization via information theory. *IEEE Trans. Knowl. Data Eng.*, 22(11):1623–1636, 2010.
17. S. Rizvi and J. R. Haritsa. Maintaining data privacy in association rule mining. In *VLDB 2002, Proceedings of 28th International Conference on Very Large Data Bases, August 20-23, 2002, Hong Kong, China*, pages 682–693. Morgan Kaufmann, 2002.
18. P. Samarati and L. Sweeney. Generalizing data to provide anonymity when disclosing information (abstract). In A. O. Mendelzon and J. Paredaens, editors, *PODS*, page 188. ACM Press, 1998.
19. J. Soria-Comas and J. Domingo-Ferrer. Probabilistic k-anonymity through microaggregation and data swapping. In *FUZZ-IEEE*, pages 1–8. IEEE, 2012.
20. L. Sweeney. *k*-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.
21. R. C.-W. Wong, J. Li, A. W.-C. Fu, and K. Wang. (alpha, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing. In T. Eliassi-Rad, L. H. Ungar, M. Craven, and D. Gunopulos, editors, *KDD*, pages 754–759. ACM, 2006.

A Proof of Theorem 1

Let $\tau_1, \tau_2 \in \mathcal{T}$ be arbitrary private tables differing by one record (i.e., one and only one $r \in \mathcal{R}$ exists and satisfies $[\tau_1(r) \neq \tau_2(r)]$ and $\tau_1|_{\mathcal{R} \setminus \{r\}} = \tau_2|_{\mathcal{R} \setminus \{r\}}$) and let $\tau' \in \mathcal{T}'$ be an arbitrary randomized table.

The proposition we should show is the following inequality.

$$\max_{\tau_1, \tau_2, \tau'} \frac{\Pr[\Delta(\tau_1) = \tau']}{\Pr[\Delta(\tau_2) = \tau']} \leq \exp(\varepsilon) = \max_{\substack{u, v \in \mathcal{V} \\ v' \in \mathcal{V}'}} \frac{A_{u, v'}}{A_{v, v'}}$$

The left-hand side of the above inequality is transformed as follows.

$$\begin{aligned}
& \max_{\tau_1, \tau_2, \tau'} \frac{\Pr[\Delta(\tau_1) = \tau']}{\Pr[\Delta(\tau_2) = \tau']} \\
&= \max_{\tau_1, \tau_2, \tau'} \frac{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \frac{1}{|\mathcal{R}|} \prod_{s \in \mathcal{R}} \Pr[(\Delta(\tau_1))(s) = \tau'(\pi(s))]}{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \frac{1}{|\mathcal{R}|} \prod_{s \in \mathcal{R}} \Pr[(\Delta(\tau_2))(s) = \tau'(\pi(s))]} \\
&= \max_{\tau_1, \tau_2, \tau'} \frac{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \prod_{s \in \mathcal{R}} A_{\tau_1(s), \tau'(\pi(s))}}{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \prod_{s \in \mathcal{R}} A_{\tau_2(s), \tau'(\pi(s))}} \\
&= \max_{\tau_1, \tau_2, \tau'} \frac{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \left(\prod_{s \neq r} A_{\tau_1(s), \tau'(\pi(s))} \right) A_{\tau_1(r), \tau'(\pi(r))}}{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} \left(\prod_{s \neq r} A_{\tau_2(s), \tau'(\pi(s))} \right) A_{\tau_2(r), \tau'(\pi(r))}} \tag{8}
\end{aligned}$$

Now, let v_1, v_2 and $\bar{\tau}$ be $\tau_1(r), \tau_2(r)$ and $\tau_1|_{\mathcal{R} \setminus \{r\}} (= \tau_2|_{\mathcal{R} \setminus \{r\}})$, respectively. Note that these three variables determine τ_1 and τ_2 uniquely. Furthermore, let $a_{\pi, v_2, \tau'}, b_{\pi, v_1, \tau'}$ and $x_{\pi, \bar{\tau}, \tau'}$ denote $A_{\tau_2(r), \tau'(\pi(r))}, A_{\tau_1(r), \tau'(\pi(r))}$ and $\prod_{s \neq r} A_{\tau_1(s), \tau'(\pi(s))} (= \prod_{s \neq r} A_{\tau_2(s), \tau'(\pi(s))})$, respectively. Using these representations, we denote the above formula with the following formula.

$$\begin{aligned}
(8) &= \max_{\tau_1, \tau_2, \tau'} \frac{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} b_{\pi, v_1, \tau'} x_{\pi, \bar{\tau}, \tau'}}{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} a_{\pi, v_2, \tau'} x_{\pi, \bar{\tau}, \tau'}} \\
&= \max_{\bar{\tau}, v_1, v_2, \tau'} \frac{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} b_{\pi, v_1, \tau'} x_{\pi, \bar{\tau}, \tau'}}{\sum_{\pi: \mathcal{R} \rightarrow \mathcal{R}} a_{\pi, v_2, \tau'} x_{\pi, \bar{\tau}, \tau'}} \tag{9}
\end{aligned}$$

By fixing v_1, v_2 and τ' , we can apply Lemma 3 to remove $\bar{\tau}$ and $x_{\pi, \bar{\tau}, \tau'}$ from the above maximum.

$$\begin{aligned}
(9) &= \max_{v_1, v_2, \tau', \pi} \frac{b_{\pi, v_1, \tau'}}{a_{\pi, v_2, \tau'}} \\
&\leq \max_{v_1, v_2, \tau', \pi} \frac{A_{\tau_1(r), \tau'(\pi(r))}}{A_{\tau_2(r), \tau'(\pi(r))}} \leq \max_{\substack{u, v \in \mathcal{V} \\ v' \in \mathcal{V}}} \frac{A_{u, v'}}{A_{v, v'}} \tag{10}
\end{aligned}$$

□